Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233
	)	

REPLY COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

Rachel S. Nemeth
Senior Director, Regulatory Affairs

Mike Bergman
Vice President, Technology & Standards

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233
	)	

REPLY COMMENTS OF
THE CONSUMER TECHNOLOGY ASSOCIATION

I. INTRODUCTION AND SUMMARY

The Consumer Technology Association ("CTA")[1] submits reply comments on the Notice of Proposed Rulemaking ("*NPRM*") and Notice of Inquiry (*"NOI*") in the above referenced dockets.[2] In the *NPRM* and *NOI*, the FCC highlighted serious concerns about untrusted equipment threatening America's communications networks. Resilient and secure networks and supply chains for communications equipment are vital to the 5G future. CTA agrees that companies posing a national security risk to U.S. networks should face serious consequences. CTA shares the Commission's goals of protecting against national security threats to the communications supply chain and promoting the integrity of connected devices. The Commission should carefully consider some of the challenges raise by proposals in the *NPRM* and *NOI* before making changes that could have wide-ranging effects across the tech industry.

---

[1] As North America's largest technology trade association, CTA® is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®—the most influential tech event on the planet.

[2] Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, *Notice of Proposed Rulemaking and Notice of Inquiry*, FCC 21-73, ET Docket No. 21-232 (June 17, 2021) ("*NPRM*" and "*NOI*").

As responsible entities in the tech sector, CTA's members take supply chain integrity and device security seriously. CTA and its members develop standards and practices to support secure networks and products. By developing risk-based industry guidance, contributing to government work on security, and leading private sector certification programs, CTA has demonstrated its commitment to device security. The record in this proceeding illustrates the proactive approaches taken by the tech industry to build security into communications networks from the ground up.[3] These efforts should be supported as technologies and threats evolve.

Commenters support ensuring the security of connected devices but raise concerns about some of the sweeping changes to the equipment authorization process discussed in the *NPRM* and *NOI*. In determining how to proceed, the Commission should consider the full implications of actions contemplated in the *NPRM* and *NOI*, including on the efficiency of the equipment authorization regime and the potential to impede technological innovation. With respect to the *NPRM*, the FCC should ensure that any next steps are legally sound, targeted at Covered List companies,[4] and avoid unintended consequences for the United States technology industry. On cybersecurity, the FCC should heed the recommendations laid out in the CTA White Paper[5] about how the government can promote secure connected devices. The agency should not

---

[3] *See, e.g.* Comments of the Consumer Technology Association, ET Docket No. 21-232, EA Docket No. 21-233 at 4-8 (filed Sept. 20, 2021) ("CTA Comments"); Comments of CTIA, ET Docket No. 21-232, EA Docket No. 21-233 at 3-6 (filed Sept. 20, 2021) ("CTIA Comments"); Comments of the Telecommunications Industry Association, ET Docket No. 21-232, EA Docket No. 21-233 at 17-19 (filed Sept. 20, 2021) ("TIA Comments").

[4] FCC, List of Equipment and Services Covered by Section 2 of the Secure Networks Act, https://www.fcc.gov/supplychain/coveredlist (Mar. 12, 2021) ("Covered List").

[5] CTA, *Smart Policy to Secure Our Smart Future How to Promote a Secure Internet of Things for Consumers* at 6 (Mar. 2021) available at: https://www.cta.tech/Resources/Newsroom/Media-Releases/2021/March/IOT-Device-Security-White-Paper-Release ("White Paper").

impose government mandates. The government should promote security by using industry-driven solutions that can adapt to the pace of innovation in a way that regulation cannot.

II. ALTHOUGH THE FCC IDENTIFIES CRITICAL NATIONAL SECURITY ISSUES, THE RECORD DEMONSTRATES THAT SOME *NPRM* PROPOSALS POSE IMPLEMENTATION CHALLENGES.

A. Security Is an Essential Component of Our 5G Future.

The security of our nation's communications networks is critical to continued American leadership in communications technology, including 5G wireless services and the Internet of Things ("IoT"). The federal government as a whole should remain focused on how to identify and root out bad actors, and the Commission should continue to consider how it can contribute to this effort, consistent with its authority and expertise.

As it considers next steps, the Commission should remain tightly focused on the national security concerns that motivated the *NPRM*. The FCC is rightly concerned about the entities included on the Covered List, which have been determined by national security experts to pose a threat to our communications networks. CTA applauds the meaningful actions the FCC has already taken to secure our communications networks from those entities in the rip and replace proceeding. With a clear mandate and $1.895 billion in funding from Congress, the FCC instituted a robust program to address threats to the security of our nation's communications networks posed by Covered List entities by reimbursing eligible providers for removing and replacing insecure equipment.[6] This program is an excellent example of how the FCC can help to safeguard the security of our nation's communications networks, and the record in response to

[6] *See NPRM* ¶¶ 14-15 (discussing *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821 (2020) and *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Second Report and Order, 35 FCC Rcd 14284 (2020)).

the *NPRM* shows strong support for the FCC's efforts in that proceeding.[7] As one commenter explained, "the Commission has important authority … that provide[s] it ample ways to help secure the communications supply chain without subjecting industry to multiple cybersecurity and software compliance regimes or establishing the dangerous precedent of rescinding existing equipment authorization."[8]

B. The Record Demonstrates that Some of the Approaches Discussed in the *NPRM* Could Stifle Innovation, and Harm Consumers.

While the *NPRM* is rightly aimed at reducing security threats from certain potential threats or bad actors, addressing network security through the equipment authorization process as the FCC has proposed could create implementation and compliance challenges for all participants in the process. This is particularly the case for proposals to revoke existing authorizations and make changes to the Supplier Declaration of Conformity ("SDoC") process, which will affect far more than the Covered List entities.

As CTA explained, the *NPRM*'s proposal to revoke existing equipment authorizations for Covered List equipment is problematic, as it "promises to create potentially massive inconvenience and cost to consumers and impose vast expense on manufacturers and others to source and install replacement equipment."[9] Numerous commenters agree that the revocation

---

[7] *See* CTIA Comments at 12 ("The Commission should be careful not to slow or undermine the important work of its rip and replace program."); Letter from ACT – the App Association, Consumer Technology Association, Council to Secure the Digital Economy, CTIA, Internet Association, Information Technology Industry Council, U.S. Chamber of Commerce, and USTelecom to Marlene H. Dortch, Secretary, FCC, ET Docket No. 21-232, at 1 (filed Sept. 20, 2021) ("Industry Letter"); TIA Comments at 2.

[8] Comments of 5G Americas, ET Docket No. 21-232, at 2 (filed Sept. 20, 2021) ("5G Americas Comments").

[9] CTA Comments at 14.

proposal entails severe challenges and complexities.[10] Given the breadth of its potential reach, revocation of existing authorizations could set "dangerous precedent,"[11] "risk jeopardizing supply chains and undermining innovation,"[12] and create "unprecedented and virtually insurmountable" compliance challenges.[13] This may undermine the reliability of the authorization process. Commenters were concerned that "outlawing already-approved equipment" would significantly impact communications companies' and consumers' investment in equipment, and irrevocably damage faith in "the stability and effect of the Commission's Part 2 approval process."[14]

Similarly, the record confirms that the *NPRM*'s proposed changes to the SDoC process could harm industry and consumers. As CTA explained, the FCC's proposed changes could foreclose use of the valuable and timesaving SDoC process by non-Covered List entities who utilize Covered List component parts. As a result, non-Covered List entities "would need to complete the more burdensome and time-consuming certification process with greater frequency—costing time and resources, and potentially deterring innovation."[15] Other commenters recognize these challenges; as one states, "[the Commission's] approach would

---

10 *See* CTIA Comments at 9-12; Comments of the Information Technology Industry Council, ET Docket No. 21-232, at 5-10 (filed Sept. 21, 2021) ("ITI Comments"); Comments of NCTA – The Internet and Television Association, ET Docket No. 21-232, at 9-12 (filed Sept. 20, 2021) ("NCTA Comments"); TIA Comments at 12.

11 5G Americas Comments at 2-3

12 CTIA Comments at 10.

13 ITI Comments at 8.

14 NCTA Comments at 10; *see also, e.g.*, ITI Comments at 6 ("Carrying out revocation in the manner proposed by the Commission would likely diminish the value of an FCC equipment authorization by calling into question whether *any* authorization could be revoked at any time, for reasons other than those currently established in law[.]") (emphasis in original).

15 CTA Comments at 19.

necessarily burden *all* who rely on the SDoC process with heavy new diligence requirements, including with respect to identifying the source of every component part, no matter how miniscule, or even software."[16] The result of the SDoC and other proposed changes to the equipment authorization regime thus could "go beyond a narrow and prospective limitation on equipment authorization for Covered companies,"[17] instead harming non-Covered List entities, the consumers they serve, and American innovation.

While the Commission rightly examines the wisdom of accepting Covered List entities to the United States' equipment authorization regime, the FCC should scrutinize potential changes to the process and consider the implications for the complex global supply chain as well as economic, policy, and legal impacts.

III. THE FCC'S EQUIPMENT AUTHORIZATION PROCESS IS NOT THE RIGHT PLACE TO ADDRESS THE CYBERSECURITY OF CONNECTED DEVICES.

CTA agrees with the Commission that it is enormously important that devices connecting to our nation's networks are secure and resilient. With respect to the proposals raised in the *NOI,* the record overwhelmingly shows that the Commission should not add cybersecurity requirements to the equipment authorization process. Further, commenters expressed concern that the Commission's proposals could complicate critical public and private sector partnerships on device cybersecurity. As set out in CTA's White Paper and underscored by comments in this proceeding, the Commission can best promote device security by supporting industry-driven best practices for devices rather than imposing new regulatory mandates.

A. Proposals in the *NOI* Could Impact Ongoing Public and Private Sector Work.

---

16 NCTA Comments at 15 (emphasis in original).

17 CTIA Comments at 19.

The role contemplated for the FCC in the *NOI* stands to duplicate, or possibly interfere with, other established and ongoing IoT security activities and proceedings. The record shows that a diverse range of stakeholder organizations and government agencies are already focused on this critical issue.[18] As commenters emphasized, there are a multitude of public and private efforts focused on enhancing device security and a vast amount of resources have been poured into these efforts. The Commission should allow the expert agencies that are engaged on this topic—such as the Department of Homeland Security ("DHS"), the National Institute of Standards and Technology ("NIST"), the Federal Trade Commission ("FTC") and others—to continue working with government partners, and in collaboration with consumers and industry, to provide guidance related to IoT device cybersecurity.[19]

Private sector organizations are addressing device cybersecurity in industry groups, best practices, certifications and partnering with government agencies. For example, as highlighted by CTA and others,[20] the Council to Secure the Digital Economy developed and updated its *C2 Consensus on IoT Device Security Baseline Capabilities*.[21] This private sector-led project involved many contributors, and the C2 Consensus sets out baseline expectations for device capabilities and lifecycle management which "provides important insights about securing devices and information in ways that earn consumer trust and deliver the full benefits of

---

18 *See, e.g.,* ITI Comments at 15 ("In the interest of regulatory comity, the Commission should approach the topic with great caution to avoid duplicating numerous ongoing USG efforts and adding yet another layer to an already confusing and crowded cybersecurity landscape.").

19 *See id.* at 15.

20 *See, e.g.* Comments of USTelecom—The Broadband Association, ET Docket No. 21-232, EA Docket No. 21-233, at 13 and Attachment 1-5 (filed Sep. 20, 2021) ("USTelecom Comments").

21 Council to Secure the Digital Economy, C2 Consensus on IoT Device Security Baseline Capabilities (2019) (see also 2021 Supplement) available here: https://csde.org/projects/c2-consensus/ ("C2 Consensus").

anytime/anywhere connectivity."[22] CTA continued this path by convening industry experts to convert the C2 Consensus to a formal technical standard, ANSI/CTA-2088.[23] This standard is now mapped to NISTIR 8259A via the NIST National Online Informative References Program,[24] in a clear demonstration of the ongoing public-private partnership.

Private sector and third-party security conformity assessment programs also have emerged without government mandates. Such third-party assessment and labeling programs include, among others, UL's IoT Security Rating, based on the UL MC 1376 security framework ; and Eurofins IoT device testing and the Secure Connected Device Logo [25] Commenters agree that the Commission and other policymakers should defer to existing self-attestation and conformity assessments by suppliers and vendors, as "[t]hese mechanisms are recognized and accepted by the marketplace, and industry has the requisite experience."[26]

Further, FCC regulation in this space could complicate an already expansive set of Federal activities related to device cybersecurity, many of which have helpfully drawn on industry engagement. Ongoing Federal agency activity includes DHS's Cybersecurity and Infrastructure Security Agency ("CISA") and public-private collaborations with the Information Technology Sector Coordinating Council, Communications Sector Coordinating Council, the

---

22 *See id*. at Acknowledgement.

23 *Baseline Cybersecurity Standard for Devices and Device Systems (ANSI/CTA-2088)*, (Dec. 2020) https://shop.cta.tech/products/baseline-cybersecurity-standard-for-devices-and-device-systems-cta-2088.

24 *See* NIST, Computer Security Resource Center, National Online Informative References Program, CTA-2088-to-NISTIR-8259A Informative Reference Details (Sept. 30, 2021) https://csrc.nist.gov/projects/olir/informative-reference-catalog/details/16.

25 Manufacturers can also take advantage of Eurofins testing of consumer IoT devices for compliance with the European Telecommunications Standards Institute (ETSI) standard 303 645. Eurofins, Cyber Security, Compliance, https://www.eurofinscybersecurity.com/compliance/.

26 USTelecom Comments at 17-18.

Information and Communications Technology Supply Chain Risk Management Task Force, the recently created the Joint Cyber Defense Collaborative and the Joint Cyber Planning Office, NTIA's Communications Supply Chain Risk Information Partnership program and the Commerce Department's interim final rule on Information and Communications Technology and Services transactions. [27]

The record also indicates that FCC regulation of device security may fragment or undermine urgent whole-of-government efforts directed by President Biden's May 12, 2021 *Executive Order on Improving the Nation's Cybersecurity* ("EO").[28] Commenters point to overlaps and impacts on the FTC's joint work with NIST on the consumer labeling pilot program and the National Telecommunications and Information Administration's ("NTIA") software bill of materials multi-stakeholder work, among others.[29]

The record reflects that the Commission must exercise caution in taking any action considered under the *NOI*. A diverse range of stakeholder organizations and government agencies are intently focused on this issue. As underscored above through stakeholder-led efforts, "[i]ndustry works hard to secure the IoT ecosystem and protect customers [and] has also collaborated with expert agencies like NIST to define baseline voluntary approaches to foundational IoT security and advance industry and international standardization."[30] Along with the many other commenters currently engaged in ongoing efforts to secure devices and networks,

---

27 *See, e.g.* CTIA Comments at 25, n. 73.

28 Comments of Multiple Industry Associations, ACT – The App Association, Consumer Technology Association, Council to Secure the Digital Economy, CTIA, Internet Association, Information Technology Industry Council, Telecommunications Industry Association, and USTelecom, ET Docket No. 21-232, at 2 (filed Sep. 20, 2021) ("Industry Letter (*NOI*)").

29 *See*, *e.g.* 5G Americas Comments at 8-9; *see also* CTIA Comments; ITI Comments; and USTelecom Comments.

30 CTIA Comments at 5.

CTA urges the FCC to allow expert agencies to continue to take the lead in collaborating with industry and consumer groups, and engage through interagency coordination.[31]

B. The Vast Majority of Commenters Agree That the Commission Should Not Pursue a Regulatory Approach to Cybersecurity as Discussed in the *NOI*.

As the record reflects, rather than taking a regulatory approach to IoT device cybersecurity, the FCC should complement the work of other agencies that have experience and expertise in facilitating industry-driven, voluntary, and flexible approaches to cybersecurity.

Commenters note that the FCC's equipment authorization process is not the right vehicle for addressing device cybersecurity. Addressing the cybersecurity of products is an ongoing and iterative process.[32] Commenters, involved in manufacturing, development, and sustained enhancement of device security agree that "[a] static regulatory model, with prescriptive rules requiring specific technologies or controls, is the wrong approach to cybersecurity in general, including IoT device security. First and foremost, static requirements are incompatible with the complex, dynamic, and rapidly evolving nature of cybersecurity threats."[33] Moreover, relying on device security mandates can foster a one-size-fits-all approach or oversimplify complex categories of connected devices.[34] This threatens to stifle IoT security innovation and impede

---

31 *See, e.g.* CTIA Comments at 27 ("The FCC should likewise consider how to support the workstreams of its federal partners and engage in inter-agency coordination to define voluntary standards rather than creating a fragmented regulatory approach. Inter-agency coordination at the federal level is particularly vital because any FCC activity on IoT security must take into account dynamic international issues, which underscore the need for a unified federal approach that champions flexibility and global reciprocity, so that U.S. companies can make and sell electronic devices and services globally."; *see also* ITI Comments at 15.

32 TIA Comments at 14-15.

33 CTIA Comments at 30.

34 *See, e.g.* CTIA Comments at 30 (discussing how prescriptive requirements "can do more harm than good, providing a road map for hackers and encouraging a check-the-box, compliance mindset, which does not encourage the proactive approaches required to stay ahead of bad actors.

gains to the economy associated with rapid innovation and diversity in technologies, as manufacturers try to fit products into regulatory categories so that they can identify mandates.

Commenters also point out that transforming NIST's voluntary baseline IoT device cybersecurity guidance into a regulatory mandate is inapt.[35] Flexibility to respond to risk is paramount, as "[d]ifferent devices—from low- to high-complexity, managed to unmanaged, and home to federal government-use—deployed in different environments for different use cases will need different, flexible approaches to cybersecurity."[36] NIST standards and publications are not intended to become regulation and should remain flexible and voluntary.[37] The record notes that the Commission could actually undermine NIST's cybersecurity guidance by incorporating the framework into the authorization process or moving independently of NIST, and that it should allow expert agencies to continue working with consumers and industry.[38]

Moreover, addressing cybersecurity through the equipment authorization model risks putting too much focus on device-centric capabilities, without proper consideration of the broader security context in which devices operate.").

35 *See*, *e.g.,* 5G Americas Comments at 5, responding to *NOI* at ¶ 102.

36 CTIA Comments at 28.

37 *Id.* at 31-32 ("NIST's voluntary, flexible, and risk-based guidance was not designed to be codified into regulation. NISTIR 8259 offers recommendations for certain "foundational cybersecurity activities that manufacturers should consider performing," noting that '[t]he considerations mentioned within these activities may not apply to all customers or manufacturers, but others may find the same considerations to be vital.' Similarly, the Core Baseline makes clear that it "is intended to give all organizations a starting point for IoT device cybersecurity risk management, but the implementation of all capabilities is not considered mandatory' and that '[t]he individual capabilities in the baseline may be implemented in full, in part, or not at all.'").

38 ITI Comments at 15 ("The best way for the Commission to engage on this topic is to allow expert agencies such as [NIST] and the [FTC] to continue working across the [U.S. Government], in conjunction with consumers and industry, to provide helpful guidance and processes for manufacturers.")

Further, adding device cybersecurity to the FCC's equipment authorization process could require substantial changes to the existing regime and place new and overwhelming burdens on the FCC. Commenters note that the FCC may lack relevant experience and resources to address cybersecurity of hardware, software, and networks.[39] Additionally, a regulatory approach to device cybersecurity by the FCC could have other unintended consequences such as creating the potential "for increased civil or regulatory liability unrelated to the improvement of device security"[40] and causing manufacturing delays, leading "to slowdowns in product development, ultimately harming companies seeking to deploy products and security solutions in a global marketplace."[41] For these and other reasons, commenters—including former FCC officials—recommend that the Commission promote IoT security through initiatives that do not disrupt the equipment authorization process.[42]

C. Commenters Point to CTA's White Paper as Sound Policy for Promoting Innovation and Improving Device Security.

The record supports the policies and principles outlined in CTA's White Paper, which illuminates how government can best promote secure connected devices and avoid regulatory missteps.[43] Government cybersecurity mandates, including certification and labeling

---

39 Industry Letter (*NOI*) at 3 ("New cybersecurity requirements would require capabilities outside the traditional role of the Office of Engineering and Technology ("OET") and a retooling of operations just as OET faces skyrocketing demand in the number and complexity of devices seeking certification. As CTA explained in its White Paper, OET will not have adequate resources to regulate cybersecurity of the connected device market, a subject that is well outside the agency's existing expertise.").

40 ITI Comments at 14.

41 USTelecom Comments at 19.

42 Comments of Jennifer Tatel and Clete Johnson, ET Docket No. 21-232, EA Docket No. 21-233, at 5 (filed Sep. 14, 2021) ("Tatel and Johnson Comments").

43 White Paper.

requirements, are misguided. Industry-driven solutions are addressing security and adapting to the pace of innovation in a way that government rulemaking cannot. New regulations that mandate the use of certain standards or that require certifications about security practices are likely to require the creation of a large bureaucracy to oversee and enforce, and they promise to have significant unintended consequences.

Multiple associations representing hundreds of global innovators, including "the breadth of the American and trusted allies' communications and technology industries" support industry-driven best practices and creative partnerships with the private sector to improve consumer IoT security.[44] CTA agrees with the importance of improving "trust through the adoption of cybersecurity best practices in consumer devices."[45] As the record reflects, "the Commission should recognize that a flexible, risk-based, and voluntary approach to device security and adoption of international and industry standards will yield the best results in securing IoT devices and protecting networks and end users."[46]

D. The FCC Can Take a Meaningful Role in Advancing the Cybersecurity of Connected Devices Through Other Means.

Commenters recognize that existing FCC advisory bodies are well-positioned to address device cybersecurity. The record underscores that the FCC's Communications Security, Reliability, and Interoperability Council ("CSRIC") would be a natural fit to study questions posed by the *NOI*.[47] The CSRIC's diverse membership, which now includes DHS, could make

---

44 Industry Letter (*NOI*) at 1, 2.

45 *NOI* at ¶ 98.

46 CTIA Comments at 23.

47 *See, e.g.,* Industry Letter (*NOI*) at 2 ("Inserting new cybersecurity mandates into the FCC's equipment authorization regime is not the right path; IoT security and the proper role of the FCC present challenges that would be best addressed in a venue like the FCC's CSRIC.");

recommendations on industry best practices, standards, and voluntary certifications that will advance IoT cybersecurity. CSRIC VIII's charter could be amended to create a working group tasked with this effort. The FCC might also consider tasking the Technological Advisory Council ("TAC") with analyzing certain technical aspects of device cybersecurity. In 2015, the TAC was asked to "examine the special cybersecurity challenges posed by the emerging Internet of Things, and to suggest actionable recommendations to the FCC with focus on the security and protection of IoT consumer products."[48] This work could potentially be updated and refreshed.

The record indicates that the FCC should embrace and promote a risk-based unified federal approach, led by expert agencies, rather than regulate in this space.[49] The Commission can contribute to IoT cybersecurity by supporting "the workstreams of its federal partners and engag[ing] in inter-agency coordination to define voluntary standards rather than creating a fragmented regulatory approach."[50] Interagency coordination is especially important because any FCC activity on IoT security "must take into account dynamic international issues, which underscore the need for a unified federal approach that champions flexibility and global reciprocity, so that U.S. companies can make and sell electronic devices and services globally."[51] Beyond this, the FCC could support education about IoT device security for the communications sector and consumers, in cooperation with NIST and the FTC.[52]

---

see also, 5G Americas Comments at 12; CTIA Comments at 33-34; TIA Comments at 17-19; and Tatel and Johnson Comments at 6.

48 FCC, TAC, Technical Considerations White Paper: Applying Security to Consumer IoT Devices, at 4 (2015), https://transition.fcc.gov/oet/tac/tacdocs/reports/2015/FCC-TAC-Cyber-IoT-White-Paper-Rel1.1-2015.pdf.

49 CTIA Comments at 6-7.

50 *Id.* at 27; *see also* USTelecom Comments at 12.

51 CTIA Comments at 27.

52 *Id.* at 34.

E. The FCC Should Not Move to an NPRM on IoT Cybersecurity.

The complex device cybersecurity topics raised in the *NOI* are not ripe for proceeding to an NPRM. The questions teed up in the *NOI* are "nebulous" and "far-reaching" and worthy of further development and consideration before moving to proposed rules.[53] It would be logical to separate the workstreams involved with the *NPRM* and *NOI* as "the *NPRM* and *NOI* involve vastly different sets of legal, technical and policy considerations."[54] The Commission need not rush to impose regulatory mandates with widespread consequences, particularly where industry and other agencies are collaborating on effective approaches to device security.

IV. CONCLUSION

The record illustrates that the tech industry, including CTA and its members, shares the Commission's goals of protecting against national security threats to the communications supply chain and promoting the integrity of connected devices. While companies posing threats to our nation's communications networks should face severe consequences, CTA urges the Commission to carefully consider the impacts of some proposals in the *NPRM* before instituting sweeping changes. With respect to the *NOI*, the Commission should pursue alternatives to support device cybersecurity without imposing cybersecurity requirements in the equipment authorization process.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: */s/*

Rachel S. Nemeth

---

53 TIA Comments at 3-4.

54 USTelecom Comments at 5.

Senior Director, Regulatory Affairs

Mike Bergman
Vice President, Technology & Standards

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202

October 18, 2021